UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/525,260	02/22/2005	Christopher Douglas Blair	762301-1560	4998

75158 7590 12/16/2009

Lawrence A. Aaronson, P.C.
Lawrence A. Aaronson
12850 Highway 9
Suite #600 PMB 338
Alpharetta, GA 30004

EXAMINER	
SANDERS, STEPHEN	

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
12/16/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

LARRY@AARONSON.COM
karscas88@hotmail.com

Office Action Summary	Application No.	Applicant(s)	
	10/525,260	BLAIR, CHRISTOPHER DOUGLAS	
	Examiner	Art Unit	
	STEPHEN SANDERS	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-14 and 17-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-14 and 17-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action has been issued in response to the RCE filed November 09, 2009 referencing the Amendment After Final to the Claims, and Remarks filed on October 06, 2009. Claims 1-2, 4-14 and 17-22 are currently pending (claim 3 is cancelled; and 1 and 13 are amended) in which claims 1, 13, and 17 are in independent form.

Status of Claims:

Claims 1-2, 4-14 and 17-22 are rejected under 35 U.S.C. 102(b).

Response to Amendment

Applicant's October 06, 2009 Amendment After Final to the Claims have been received and entered, in which claims 1 and 13 are amended.

Response to Arguments

Applicant's arguments filed October 06, 2009 have been fully considered and are not persuasive as they relate to 35 U.S.C. 102. Applicant's argument regarding the amended claims state that there is no teaching or suggestion of including "encrypted search conditions within the decryption keys" in Van Oorshot. Examiner disagrees and has shown additional references within Van Oorshot that teach or suggest this feature. As such, Applicant's argument has been fully considered and is not persuasive. Applicant's claim amendments have been entered. Accordingly, as stated above, the rejections remain and are shown below in greater detail with respect to the amended claims.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-14 and 17-22 rejected under 35 U.S.C. 102(b) as being anticipated by Van Oorshot et al U.S. Patent Number 6,229,894; Date of Patent: May 8, 2001 hereinafter Van Oorshot.

As to claim 1, the following is taught: "a method for monitoring (Van Oorshot: column 2, lines 4-10 indicate the needs of the law enforcement agencies in the monitoring of communications) of communications traffic, comprising: connecting a recorder to a network switch to record packet-data communication traffic received from, and passing through, the network switch";

"encrypting the packet-data communication traffic at an encryption engine communicatively connected to the recorder after the packet-data communication traffic has passed through the network switch to create encrypted data" (Van Oorshot: column 5, lines 56-65 – also see encrypted transmission (ciphertext) 54 in Figure 2 which includes the signature of sending end-user 56, the encrypted file or message 58, and the wrapped session key 52); and

"storing the encrypted data (Van Oorshot: Figure 1, and its description starting in column 3, line 15 discloses the receiving, encrypting, recording, and storing of communications data as well as a decryption key required for its decoding) in a storage

device such that the encrypted data can be decrypted only by means of decryption keys that exhibit restricted availability" (Van Oorshot: column 4 line 59 to column 5, line 5),

"wherein encrypted search conditions are included within the decryption keys" (Van Oorshot: column 3, lines 1-15; column 7, lines 31-61, to access user specific encryption information).

As to claim 2, the following is taught: "the method as claimed in claim 1 further including employment of a spare disk and/or CPU capacity within a telecommunications system" (Van Oorshot: column 7, lines 17-30).

As to claim 3: cancelled.

As to claim 4, the following is taught: "the method as claimed in claim 1, further including the step of employing separate levels of authorization for access to the stored data" (Van Oorshot: column 3, lines 1-8; column 7, lines 31-42).

As to claim 5, the following is taught: "the method as claimed in claim 1, further including the step of employing a decryption key that is useable only once" (Van Oorshot: column 7, line 55-57; column 8, lines 21-39, and lines 45-51).

As to claim 6, the following is taught: "the method as claimed in claim 1, further including the step of logging" (Van Oorshot: Abstract, column 1, lines 60-67 discloses

identity authentication of requestor) "all accesses to the stored data to an encrypted secure audit trail" (Van Oorshot: column 3, line 57 to column 4, line 5; column 5, lines 56-65).

As to claim 7, the following is taught: "the method as claimed in claim 1, further including a tamper detection reference within the encrypted data" (Van Oorshot: column 4, lines 23-67).

As to claim 8, the following is taught: "the method as claimed in claim 1, further including the step of monitoring all the available communications traffic" (Van Oorshot: column 2, lines 4-14, disclose the problem for law enforcement agencies to obtain wire-tap information; column 10, lines 43-52 disclose the legal capability of law enforcement agencies to monitor and record unlimited information for its lawful and potential future scrutiny).

As to claim 9, the following is taught: "the method as claimed in claim 8, wherein the step of storing the recorded traffic comprises the step of recording all of the recorded traffic" (Van Oorshot: column 2, lines 4-14, disclose the problem for law enforcement agencies to obtain wire-tap information; column 10, lines 43-52 disclose the legal capability of law enforcement agencies to monitor and record unlimited information for its lawful and potential future scrutiny).

As to claim 10, the following is taught: "the method as claimed in claim 1, wherein the communications traffic to be recorded comprises traffic through a telecommunications switch, router or gateway" (Van Oorshot: column 3, lines 15-32; column 3, lines 16-39).

As to claim 11, the following is taught: "the method as claimed in claim 1, further including the step of encrypting details relating to the communications traffic and storing the said encrypted details for subsequent access" (Van Oorshot: Figure 2, and column 5, line 28 to column 8, line 6).

As to claim 12, the following is taught: "the method as claimed in claim 1, further including the step of authorizing use of the required decryption key in a restricted manner" (Van Oorshot: Figure 3, and column 8, lines 7-59).

As to claim 13, the following is taught: "a system for monitoring of communications traffic, comprising":

"a recorder that records the communications traffic, the communications traffic being received by the recorder from a network switch; an encryption engine that encrypts the communications traffic after the communications traffic has passed through the network switch to the recorder" (Van Oorshot: column 5, lines 56-65 – also see encrypted transmission (ciphertext) 54 in Figure 2 which includes the signature of sending end-user 56, the encrypted file or message 58, and the wrapped session key

52; also see server 16, processing device 90, memory 92 of Figure 2, and column 7, lines 17-27), and

"a storage device that stores recorded communications traffic as encrypted data, such that the encrypted data can be decrypted only by means of keys that exhibit restricted availability" (Van Oorshot: see secure storage of users' decryption private keys of server 16 in Figure 2, and column 7, lines 27-30; and directory 68 (a database) of Figure 2, and column 6, lines 50-54),

"wherein encrypted search conditions are included within the decryption keys" (Van Oorshot: column 3, lines 1-15; column 7, lines 31-61, to access user specific encryption information).

As to claim 14, the following is taught: "the system as claimed in claim 13 further including application software and executes the method steps of any one or more of claims 2-12" (See Van Oorshot's teachings above with regards to claim 13, and specifically with regards to claims 2-12).

As to claim 15: (cancelled).

As to claim 16: (cancelled).

As to claim 17, the following is taught: "a method for monitoring of communications traffic, comprising the steps of:"

"receiving communications traffic from a network switch; encrypting the communications traffic after the packet-data communication traffic has passed through the network switch" (Van Oorshot: column 5, lines 56-65 – also see encrypted transmission (ciphertext) 54 in Figure 2 which includes the signature of sending end-user 56, the encrypted file or message 58, and the wrapped session key 52) "to generate encrypted communications traffic data" (Van Oorshot: Figure 1, and its description starting in column 3, line 15 discloses the receiving, encrypting, recording, and storing of communications data as well as a decryption key required for its decoding);

"storing the encrypted communications traffic data in a storage device" (Van Oorshot: see server 16, processing device 90, memory 92 of Figure 2, and column 7, lines 17-27) "such that the encrypted communications traffic data can be decrypted by decryption keys that exhibit restricted availability, that allow encrypted search conditions and that employ separate levels of authorization for access to the stored data" (Van Oorshot: see secure storage of users' decryption private keys of server 16 in Figure 2, and column 7, lines 27-30; and directory 68 (a database) of Figure 2, and column 6, lines 50-54); and

"encrypting details relating to the communications traffic and storing the said encrypted details for subsequent access" (Van Oorshot: see sending end-user 18, and end-user encryption certificate of end-user 60, 62, 64 in Figure 2, and column 5, lines 39-55).

As to claim 18, the following is taught: "the method as claimed in claim 17, further including the step of employing a decryption key that is useable only once" (Van Oorshot: column 8, lines 21-39).

As to claim 19, the following is taught: "the method as claimed in claim 17, further including the step of logging" (Van Oorshot: Abstract, column 1, lines 60-67 discloses identity authentication of requestor) "all accesses to the stored data to an encrypted secure audit trail" (Van Oorshot: column 3, line 57 to column 4, line 5; column 5, lines 56-65).

As to claim 20, the following is taught: "the method as claimed in claim 17, further including a tamper detection reference within the encrypted data" (Van Oorshot: column 4, lines 23-67).

As to claim 21, the following is taught: "the method as claimed in claim 17, further including the step of monitoring all the available communications traffic" (Van Oorshot: column 2, lines 4-14, disclose the problem for law enforcement agencies to obtain wire-tap information; column 10, lines 43-52 disclose the legal capability of law enforcement agencies to monitor and record unlimited information for its lawful and potential future scrutiny).

As to claim 22, the following is taught: "the method as claimed in claim 17, wherein the step of storing the recorded traffic comprises the step of recording all of the recorded traffic" (Van Oorshot: column 2, lines 4-14, disclose the problem for law enforcement agencies to obtain wire-tap information; column 10, lines 43-52 disclose the legal capability of law enforcement agencies to monitor and record unlimited information for its lawful and potential future scrutiny).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephen Sanders whose telephone number is 571-270-5308. The examiner can normally be reached on M - F; 7:30a.m. - 5:00p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Stephen Sanders/
Examiner, Art Unit 2434
/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434